

AGNITIO



VoiceBiometricsConference

presented by  opusresearch

London

November 6-7 2013



Emilio Martinez

emartinez@agnitio-corp.com

“How to choose a Voice
Biometrics Engine”

Voice Biometrics Engines



Authentication solution vs. Voice Biometrics Engine

Selecting a VB Engine

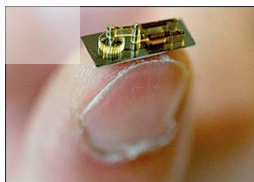
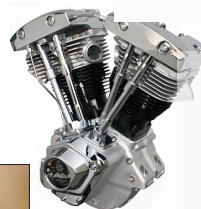
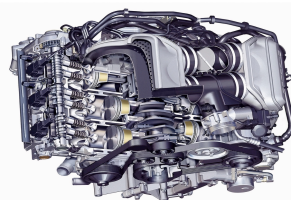
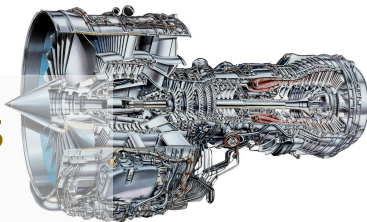
- End Users are closer to Authentication solution requirements
- Selecting the right engine is challenging and sometimes tricky
 - It requires specific expertise, sometimes far from End User or Solution Provider expertise.
 - It **drains resources and time** when done correctly

*AGNITIO is a company that sells engines. The following might be biased. But the problem described here **affects all of us**. Other industries have found ways to make engine evaluations more effectively.*

Selecting the VB Engine you need



- Natural Speech, pass phrase, or both
- Match on device, match on server, or both



Engine Options

Streaming, Speaker Separation, 1:N optimization..

Engine capabilities are evolving quickly. New engine models and options can enable new features in Authentication Solutions



“In God we trust; all others must bring data”

W.Edwards Deming

Key Metrics: the SUN



Secure

- How the engine allows you to build a strong, yet simple, authentication process

Universal

- How the engine will behave when deploying your solution in any country, using any channel

Natural

- How the engine enables natural and human friendly authentication solutions in real life environments

Secure



Accuracy

- *EER, False Acceptance vs. False Rejection*



Spoofing

- *Replay attacks, voice synthesis, Artificial signals*



Hacking.

- *Binary and memory tampering*



The more accurate the engines, the more expensive to test.

*The tests must be statistically robust.
(Doddington's rule of 30)*

Number of Speakers needed for a meaningful test

	EER 5%	EER 0.1%
# Rec/Spk = 5	60	3.000
# Rec/Spk = 10	13	650



Voice Biometrics is perceived as
easy to spoof

Hollywood, Wikipedia, Social media



WIKIPEDIA
The Free Encyclopedia



WIKIPEDIA
The Free Encyclopedia

Voice biometrics is so powerful it's
easy to spoof



Dan Miller @dnm54

22 Jan

Biometrics and Multifactor Auth (MFA) have got to replace or augment Username/passwords and KBAs. Today's solutions are madness #authchat

Details



Jeffrey Goldberg @jpgoldberg

22 Jan

Even Hollywood script writers know what's wrong with biometric authentication. "My voice is my passport"

#authchat

Details



Dan Miller @dnm54

22 Jan

The Sneakers critique has damned voice biometrics for 2 decades now. But anti-spoofing has come a long way. #authchat

Details



Jeffrey Goldberg

@jpgoldberg

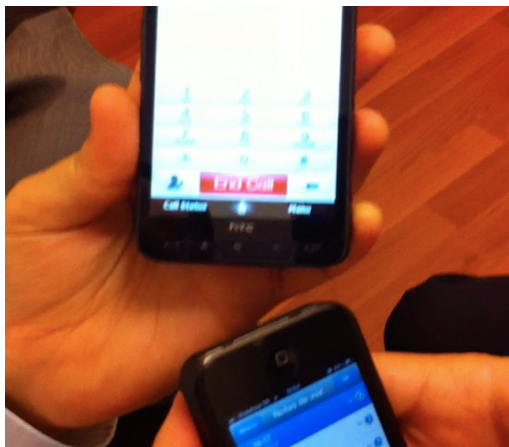


Follow

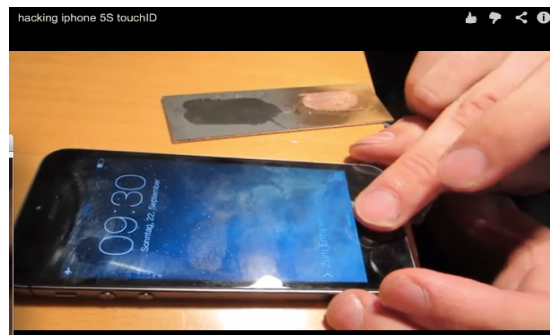
@dnm54 Spoofing biometrics has also come a long way. Each new anti-spoof mechanism may require costly new hardware. #authchat

Types of VB Spoofing

- **Replay attacks**
 - *Recording when user says the pass phrase, or with cut & paste*
- **Voice synthesis**
- **Artificial Signals**



Unpublished video of VB Spoofing in a real life deployment



YouTube video of fingerprint Spoofing for Apple 5S

- **Avoid nasty surprises after deployment with a thoroughly anti spoofing testing**
 - *Do not expect 100% protection. Measure how difficult it is to break it*
 - *Do not expect eternal protection. Asses the engine manufacturer program to improve protection with new threats*
- **It is not a conventional test.**
 - *A specialist should try different ways of attacks*



- **Mainly for match on device engines**
 - *Match on server can also have risks, but it is usually protected by the solution, not by the engine*
- **Standard tests and protection**
 - *New to Voice Biometrics Engine Manufacturers (Encryption, trustzone, match on card)*

Universal



All Channels

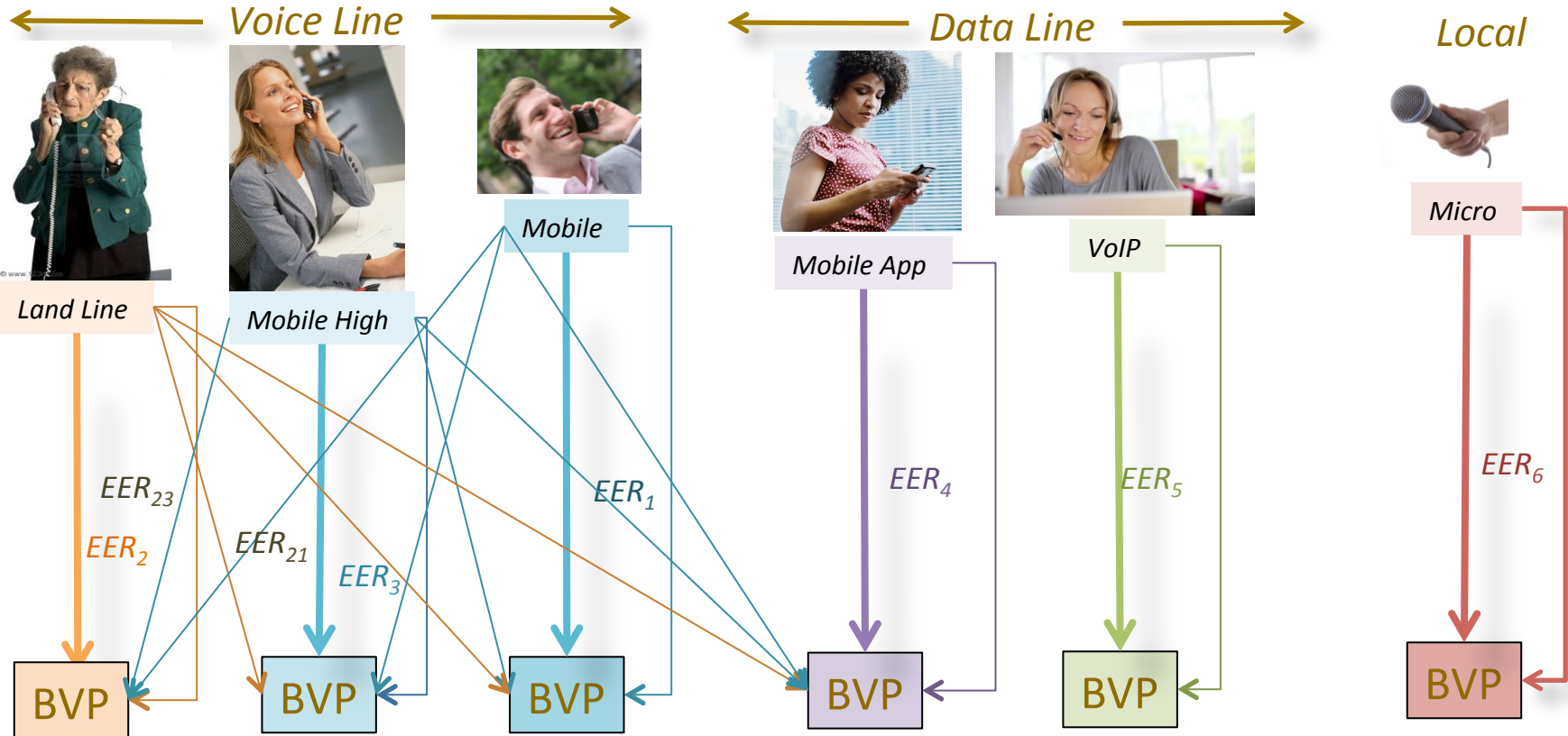


All Languages & Accents

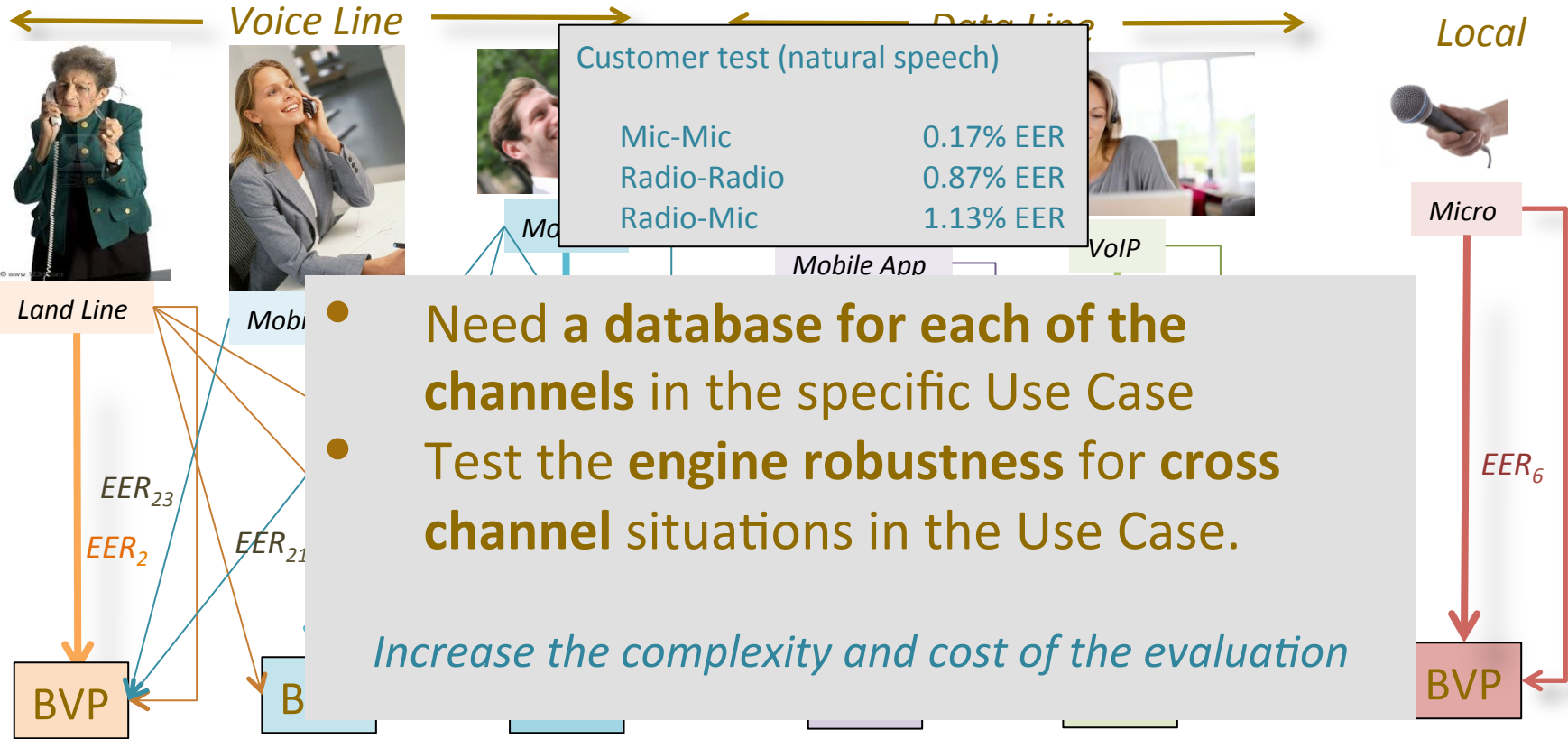


Easy Calibration & Tuning

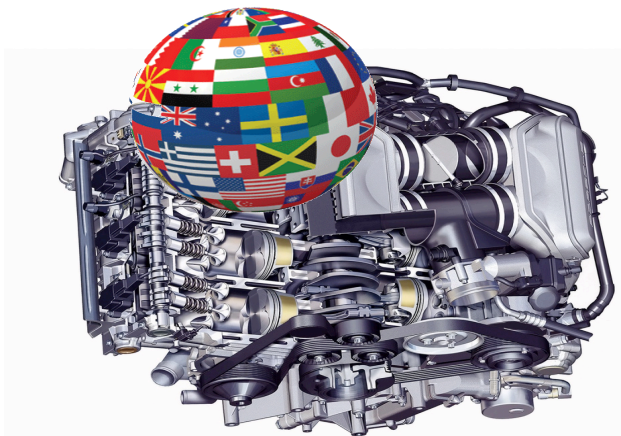
Voice Biometrics



Voice Biometrics



UNIVERSAL: Languages



New generation Engines are completely independent of the language

Other engines may require specific versions (Licenses) for each language.



- **How many languages** are available
- **Cost** of licenses and Professional services
- **Accuracy** per language
- Check strong **accent differences**

UNIVERSAL: Calibration & Tuning



All Engines improve performance with some kind of calibration and fine tuning to adapt to new deployments.

Check hidden costs to get the promised (measured) performance

Examples for Pass phrase case

- *Can the solution provider calibrate new phrases with no additional Prof Services?*
- *Can the end user select his own personal phrase without any calibration at an acceptable EER?*



Natural



Environmental Noise

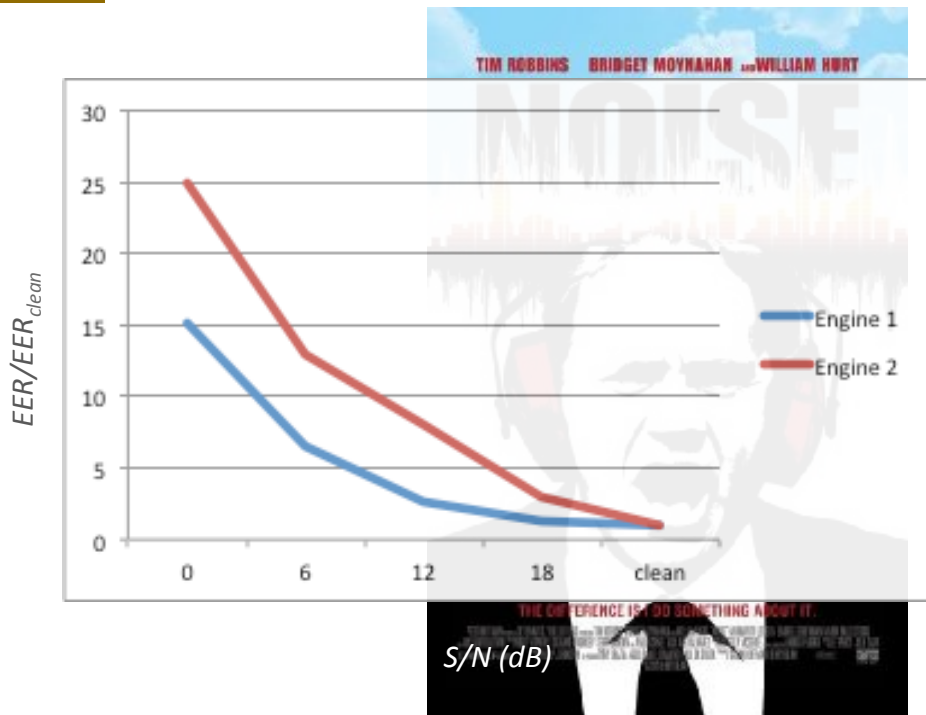


Speed & Scalability



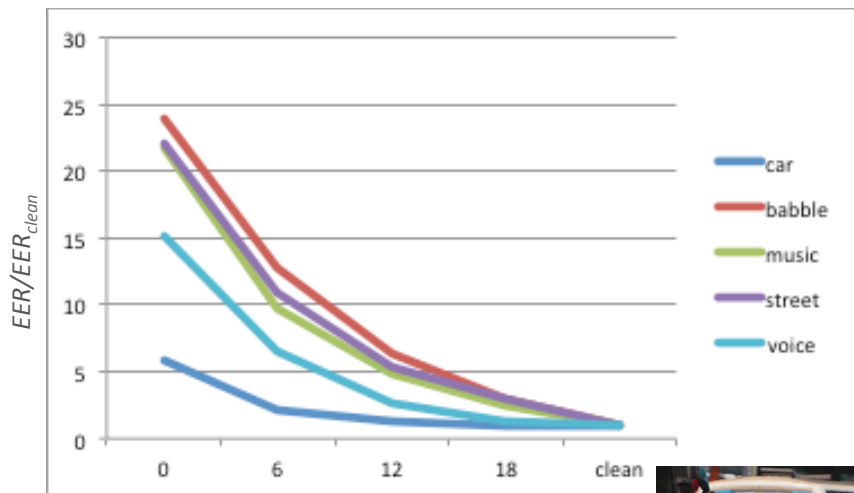
Audio Length

Voice Biometrics



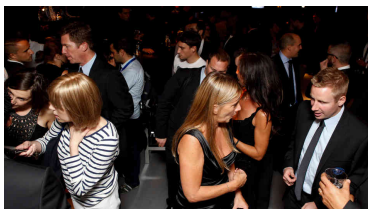
There is always a degradation of EER with noise.

Not all engines respond to noise in the same way



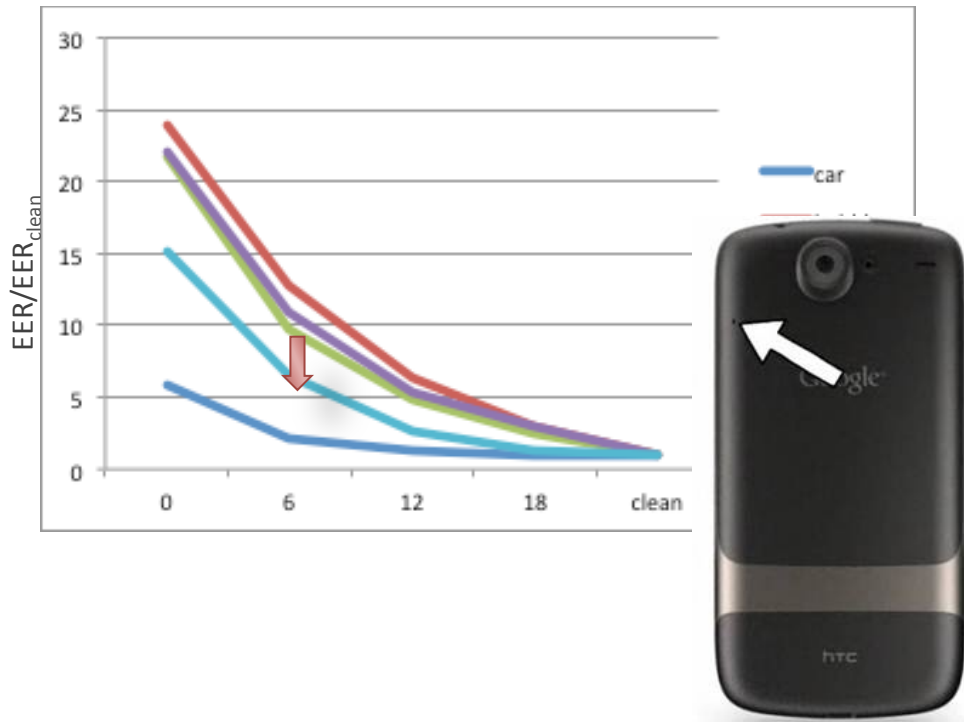
Different noise types generate different EER degradation

Create database with the appropriate noise for your use case



S/N (dB)





Some smart phones include Noise Cancellation HW/SW that can produce significant improvements

Not all engines take advantage of these Noise Cancellation technologies

NATURAL: Speed & Scalability



SPEED: Does it matter?

Engine verification speed is a hidden cost.

or..



0.2 sec/ver

0.75 sec/ver

10 CPU cores

40 CPU cores

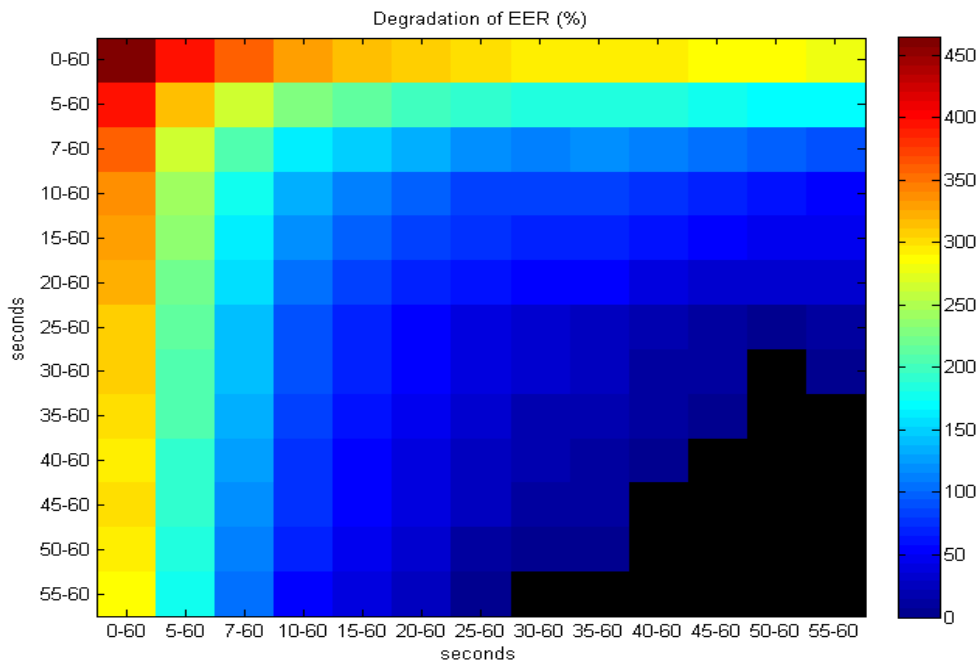
100.000 users with peaks of 50 ver/sec



We hate talking to machines and repeating phrases.

Engines that requires less audio enable more user friendly solutions





EER is VERY dependent of the quantity of audio. For enrollment and for authentication

Not all engines produce the same degradation with length



Secure

- *EER, Anti-spoofing and tampering protection*

Universal

- *Cross Channel, Language, Tuning requirements*

Natural

- *Noise resistant, Fast response, Short audios,*



Engine Manufacturers, Solution Providers and End Users will save time and money if independent trusted third parties perform periodic comprehensive Engine Evaluations.

NIST, National Physical Lab, IBG (now Novetta), CCIR, Cyara, Empirix, Tabula Rasa, iSec..



AGNITIO

Q&A

www.agnitio-corp.com